LESSON 5
INFORMATION OPERATIONS PLANNING

"Advanced technologies can make third-class powers into first-class threats."

—Vice President Dick Cheney

"I have come to realize a growing need ... to benefit from the very real potential of information operations. The Marine Corps is simply not effectively engaged and up-to-date... We must engage now to ensure our forces remain both capable and relevant into the future."

—LtGen Libutti, Former COMMARFORPAC

Lesson Introduction

The global environment coupled with the tragic events of 11 September 2001 have forever changed the world we live and fight in. We have engaged in a global war on terror; Operation Enduring Freedom was a quick and violent response that deposed the Taliban and gave Afghanistan new hopes in rising as a free nation liberated from oppression. The subsequent actions in Iraq, Operation Iraqi Freedom, removed the long, violent, and ruthless regime of Saddam Hussein. Yet, we today are continually plagued with residual threats associated with remnants of those we strove to eliminate and remove from power. The buzzword of the day heard often about the 9-11 attacks is that it was "low tech, high concept." This described the possibility that perhaps we have become overly reliant on technology for change, while perhaps underestimating the power of people and ideas to push change to get dramatic results. That dark day proved to many that the asymmetric threats from enemies we face today do not necessarily need huge resources and vast amounts of manpower to take on the world's lone superpower. Instead, the use of computers connected to the Internet, which can readily be accomplished in most parts of the world today, can provide a command and control capability in this global world that can wreak havoc on one or more of our elements of national power. We, as a nation and as a military force, must be ready to deal with this enemy that can strike us at will in a variety of ways that heretofore we hadn't foreseen or expected. As we continue to leverage and integrate emerging technologies into warfighting, we must be ready for our asymmetric foes to do likewise. We must develop strategies to gain and maintain technological superiority in dealing with these foes to keep them at bay or to defeat them.

In this lesson, we will examine the functions of information operations (IO) from both a Marine Corps and a joint perspective. We will learn the current IO capabilities, as well as look at how the MAGTF conducts IO planning to ensure IO is properly integrated into all aspects of operational and tactical planning. We will study doctrine to ensure all are versed with current philosophies and thinking within the Marine Corps and throughout the joint world. That withstanding, understand that doctrine is evolving in this volatile subject area. All should

understand that the information environment is continually changing, and, although we have attempted to provide the most current information as of this printing, the onus is on you to stay current with this evolving part of warfare.

Student Requirements by Educational Objective

Requirement 1

<u>Objective 1</u>. Explain how information and information operations (IO) will be part of every mission and the principles that are essential to successful integration of IO within the MAGTF. [JPME Area 2(a)(d), 3(a)(e), 5(a)(b)]

<u>Objective 2</u>. Describe how information operations (IO) contributes to the MAGTF in its battlespace shaping, force enhancement, and force protection efforts. [JPME Area 1(a), 2(a)(d), 5(a)(b)(d)]

> Read:

> – MCWP 3-40.4, *Marine Air-Ground Task Force Information Operations* (9 Jul 03), pp. 1-1 to 1-8 (8 pages).
> – Kuehl, Daniel T. and Neilson, Robert E., "No Strategy for the Information Age," U.S. Naval Institute, *Proceedings*, Annapolis: Sep 2003. Vol. 129, Is. 9; p. 2 (2 pages).

> Reference:

> – Lesson 7 (Introduction to Information Operations), Course 8803A (Operational Level of War)

As the nation's expeditionary force in readiness, Marines will confront many new changes in the future. For us to remain relevant, Marines must use all our capabilities to the best possible advantage. In addition to our more traditional capabilities of maneuver and firepower, our capabilities include the control, use, and exploitation of information. The rapid advance of technology has brought new capabilities as well as new challenges. As we have seen, these advantages are accompanied by new dangers. Our enemies will generally possess a regional or national level of influence and will likely have access to a variety of lethal and non-lethal technologies available on the global market.

As stated in Marine Corps Strategy 21, we can expect that regional powers, rogue elements, and non-state actors will pose security challenges embracing conventional military and non-traditional capabilities. Weapons of mass destruction, terrorist acts, and information attacks will exact an inordinate price for small lapses in the preparation of the battlespace.

Marine Corps IO supports maneuver warfare through actions that use information to deny, degrade, disrupt, destroy or influence an adversary commander's methods, means or ability to

command and control his forces and to inform target audiences through informational activities. IO is conducted during all phases of an operation, across the range of military operations, and at every level of war.

The U.S. will continue to be involved in a wide range of humanitarian and global security responsibilities, and Marines must expect to be tasked to—

- Conduct humanitarian assistance (domestic or foreign) after a disaster.
- Provide peace support for nations that seek a secure environment to peacefully develop.
- Perform peace enforcement to separate warring factions.
- Create conditions for the peaceful resolution of a crisis.
- Project combat power when resolving a crisis that requires the threat or use of force.

To project power and influence, Marine Corps forces employ for presence, engagement, and response. Each will have a strong informational component. The on-scene presence of the forward-deployed MAGTF—and its proximity and access to potential crisis areas—will establish it as a vital operational and informational cornerstone for follow-on forces acting as part of a national and theater crisis response.

The following principles are essential to the successful integration of IO within the MAGTF:

- **Integrated Function**. Integration of capabilities is a part of how Marines fight. MAGTF IO planning is conducted by a unique IO cell comprised of subject matter experts for integration into both MAGTF and joint IO plans.

- **Focused on the Objective**. Like all operations, information operations ultimately exist to help the MAGTF achieve its mission.

- **Determined IO Targets and Objectives**. The MAGTF should determine the vulnerabilities and critical elements of friendly and enemy information, information-based processes, and information systems. Likewise, the enemy will target MAGTF C2 systems, and, therefore, protection of systems critical to the MAGTF is paramount. Whether attacking or defending, IO targets and objectives are determined by the commander's intent and concept of operations.

- **Synchronized and Integrated with Higher and Adjacent Commands**. IO will be conducted in battlespace that has already been shaped by the combatant commanders' peacetime theater security cooperation events. The joint force commander (JFC) provides guidance and direction for conducting IO to support his mission, concept of operations, objectives, and intent. The MAGTF IO plan, while leveraging and exploiting the IO capabilities of higher echelons in support of MAGTF objectives, must also support the JFC's IO objectives.

- **Supported by the Total Force**. Not all IO activities that support the MAGTF are conducted by the MAGTF. For instance, Marine Corps Reserve forces provide some unique assistance (for example, civil affairs), and the MAGTF may have to conduct reach back for some of this support.

- **Developed as a Coherent Strategy**. The support and integration of the warfighting functions of the MAGTF (maneuver, fires, logistics, force protection, intelligence, and C2), as well as the design and operation of information systems, is critical to the successful conduct of IO.

- **Supported by Intelligence**. It should be understood, but in case it bears repeating, IO requires accurate, timely, and detailed intelligence. This includes intelligence preparation of the battlespace, analysis, and assessment.

IO is conducted during all phases of an operation, across the range of military operations, at every level of war, and can span from high to low tech applications. IO will primarily support battlespace shaping, force enhancement, and force protection actions; it will further support any other information-oriented activity the MAGTF can use to tailor its application of combat power. IO is both offensive and defensive in nature.

Battlespace Shaping
Our nation seeks to shape the international environment through a variety of means, including diplomacy, economic cooperation, international assistance, security assistance, and arms control. These efforts use power, information, and influence to achieve national objectives. In peacetime, forward-deployed Marine expeditionary units (MEUs) demonstrate national resolve through forward presence, and Marines enhance regional stability through cooperative engagement with allies in exercise, exchange, and informational programs. During crises, MAGTF-shaping operations must be linked to U.S. strategic objectives and must be consistent with on-going regional engagement activities. During conflict, MAGTF-shaping operations focus on setting those conditions necessary for operational and tactical success. IO, used in support of battlespace shaping, ensures that the purpose of the MAGTF's mission is clear to both the local and the worldwide audience. It is important for all to understand that perceptions count. Many of whom we will be operating with and around, military and civilian alike, will perceive actions differently. The perceptions created by MAGTF operations will result in changes to political realities that may, in turn, affect the assigned MAGTF mission. Information is a powerful component of battlespace shaping. Not only do actions matter, but the perceptions that actions create matter. The actions of our "strategic" corporals can have international ramifications, particularly when given a certain media spin. It is imperative that all Marines are aware of this fact, and we all must consider the political, cultural, and moral aspects of the battlespace within which we are operating.

Force Enhancement
Networking and advances in computing power have improved the processing and displaying of intelligence and battlefield information. In many ways, the ability to obtain timely and accurate information has emerged as a critical aspect of C2, strategic agility, and operational maneuver. The force that best controls, uses, and safeguards information and information systems has always enjoyed a decided military advantage; this truth will not change. The human decisionmaking process is the ultimate target. At the operational level, a principal focus of IO is the enemy commander and his decisionmaking process. Actions will be oriented against C2 targets to disrupt, degrade or deny an enemy's use of information and information systems to achieve operational objectives. Employed as an integrating strategy, force enhancement

activities weave together related offensive IO capabilities and informational activities toward satisfying a stated objective.

Force Protection
Information systems enable and enhance warfighting capabilities; however, increasing dependence upon these rapidly evolving technologies may create new vulnerabilities. Management decisions will have to be made based on the anticipated requirements and information resources most needing protection. The integration of protection, detection, and reaction capabilities is needed to mitigate the effects of enemy action and environmental effects. IO will enhance force protection by protecting and defending the information and information systems that the MAGTF depends upon to conduct operations. From the force protection perspective, the basis for defensive IO planning is the conduct of OPSEC, C4 vulnerability analysis, computer network defense, identification and protection of essential elements of friendly information, and the generation of the restricted frequency list.

<div align="center">

Requirement 2

</div>

Objective 3. Identify the five information operation (IO) core capabilities of military deception (MILDEC), electronic warfare (EW), operations security (OPSEC), psychological operations (PSYOP), and computer network operations (CNO); the five IO supporting capabilities of physical attack, information assurance, physical security, counterintelligence, and combat camera; and the two IO related capabilities of public affairs and civil-military operations. Demonstrate how these capabilities, be they offensive, defensive, or informational in nature, are integrated into the concept of operations to ensure successful employment of IO in support of the MAGTF and JFC. [JPME Area 1(a)(e), 2(a)(d), 3(e), 4(e), 5(a)(b)(c)(d)]

Objective 4. Describe basic joint doctrine about the information operations (IO) cell, the IO responsibilities of MAGTF staff sections, and the functions and responsibilities of the task-organized MAGTF IO cell. [JPME Area 1(a)(e), 2(a)(d), 3(a), 5(a)(b)(c)]

Objective 5. Discuss how information operation (IO) planning is integral to the MCPP and how IO is formulated both offensively and defensively. [JPME Area 1(a)(e), 2(a)(d), 3(e), 4(a)(e), 5(a)(c)]

> Read:
> - MCWP 3-40.4, *Marine Air-Ground Task Force Information Operations*, 9 Jul 03, pp. 2-1 to 2-10, and 3-1 to 3-20 (29 pages).
> - Joint Pub 3-13, *Joint Doctrine for IO*, 9 Oct 98, pp. IV-1 to IV-9 (9 pages)
> - *Joint Information Operations Planning Handbook* (July 2003), pp. 1-4 to 1-7 and pp. A-1 to A-5 (9 pages).

IO Core Capabilities
IO is multi-disciplined and must be used together with a variety of elements in an integrated strategy. Some of these elements are more offensive, defensive or informational in nature, but it is their integration into the concept of operation that ensures successful employment of IO in support of the MAGTF. Those elements include the following:

- **Military Deception**. Military deception targets enemy decisionmakers by targeting their intelligence collection, analysis, and dissemination systems. Military deception is focused on achieving a desired behavior, not simply in misleading. Special security parameters must be implemented during deception operations due to their sensitive nature.

- **Electronic Warfare**. Electronic warfare is any military action using electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy.

- **Operations Security**. OPSEC is the key to information denial. It lets the commander identify indicators that can be observed by enemy intelligence systems. OPSEC identifies, selects, and executes measures that eliminate or reduce indications and other sources of information that the enemy may exploit to an acceptable level.

- **Psychological Operations**. At the strategic level, PSYOP may take the form of political or diplomatic positions, announcements or communiqués. At the operational level, PSYOP can include the distribution of leaflets, radio and television broadcasts, and other means of transmitting information that provides information intended to influence a selected group. The mere presence of Marine Corps forces may be a PSYOP activity in itself, bringing influence on a situation through a display of purpose. The Marine Corps has no dedicated PSYOP units. Support is requested from the Army's 4th PSYOP Group; the Air Force's EC-130E Commando Solo; and the Navy's fleet tactical readiness group.

- **Computer Network Operations**. CNO are comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations.

IO Supporting Capabilities

- **Physical Attack**. Physical attack applies friendly combat power against the enemy. It reduces enemy combat power by destroying enemy forces, equipment, installations, and networks. Within IO, physical destruction is the tailored application of combat power to achieve desired operational effects. Physical attack requires considering the systematic degradation or destruction of selected enemy C2 systems to allow the MAGTF to gain an informational advantage. ROE are critical in this aspect of IO.

- **Information Assurance**. IA protects and defends information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. IA includes information security, computer security, and COMSEC. Education, training, and awareness are critical for successful IA.

- **Physical Security**. Physical security is concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft. Physical security contributes directly to information security.

- **Counterintelligence**. The principal objective of CI is to assist with protecting friendly forces. CI is the intelligence function concerned with identifying and counteracting the threat posed by hostile intelligence capabilities and by organizations or individuals engaged in espionage, sabotage, subversion or terrorism.

- **Combat Camera**. Combat camera (COMCAM) is the term for the MAGTF's own visual information (VI) capability. It is an information resource that provides a timely, accurate, "you-are-there" imagery perspective on military operations. COMCAM is essential to internal and external communications. The need for the COMCAM and VI capabilities will increase as the Marine Corps reaches Marine families, interacts with domestic and international media, and provides tactical imagery to enhance force protection and situational awareness.[1]

IO Related Capabilities

Note that the following capabilities don't exist *specifically* to support IO. They are, however, enabling capabilities.

- **Public Affairs**. Public affairs (PA) provides timely, accurate information to Marines and the general public and initiates and supports activities contributing to good relations between the Marine Corps and the public. It speeds the flow of accurate and timely information to internal and external audiences. The challenge is to get information, both good and bad, out effectively, efficiently, and honestly. PA must be carefully separated from other informational efforts aimed at manipulating perceptions. Any deviations from the truth will destroy the credibility and effectiveness of Marine Corps PA operations.

- **Civil-Military Operations**. Through careful planning, coordination, and execution, civil-military operations (CMO) can help shape the battlespace, enhance freedom of action, isolate the enemy, meet legal and moral obligations to civilians, and provide access to additional capabilities. It can also minimize civilian interference with the mission.

The Joint IO Cell

The joint IO cell is formed from select representatives from each staff element, component, and supporting agencies responsible for integrating capabilities and related activities. This cell merges capabilities and related activities into a synergistic plan. The cell coordinates staff elements and/or components represented in the IO cell to facilitate the detailed support necessary to plan and coordinate IO. A typical joint IO cell is shown in the following diagram:

---

[1] A note about the difference between PA and COMCAM. PA exists to inform, not influence, its external audience about the Marine Corps. COMCAM is a communications tool that can support myriad tasks and missions, including PA. It provides the MAGTF its own visual information capability.
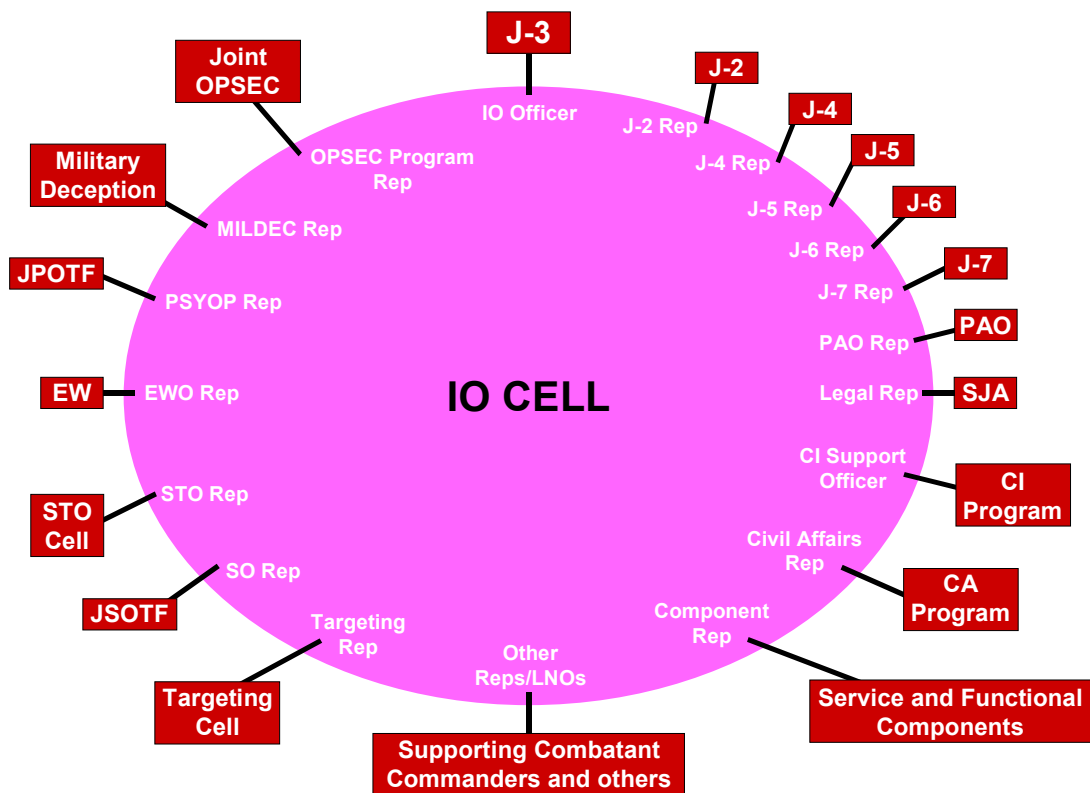
Typical Joint Information Operations Cell.

MAGTF IO Cell Organization and Functions

At the MAGTF level, the G-3/S-3 is responsible for IO. The future operations section oversees the planning and coordination of the IO effort. The G-3/S-3 will normally assign an IO officer to lead the MAGTF IO cell. The MAGTF IO officer is responsible for the following:

- Broadly integrating and synchronizing IO efforts.
- Responding directly to the G-3/S-3 for MAGTF IO.
- Ensuring that the IO cell provides input to the operational planning team (OPT) during planning to ensure coordinated operations.
- Preparing the IO appendix to the operation order (OPORD).
- Overseeing the core personnel within the IO cell as well as augmentees from external agencies.
- Ensuring that all IO matters are coordinated within the MAGTF staff, higher headquarters, and external agencies.

This IO cell is normally composed of intelligence personnel, augmentees supporting IO activities, and representatives from staff elements and subject matter experts from appropriate warfighting functions. The size and structure of the cell are tailored to meet the mission and the commander's intent. The IO cell's function is to integrate a variety of separate disciplines and functions pertaining to IO for the command. IO integration requires extensive planning and coordination among all the elements of the staff. The IO cell, when established, is a mechanism for achieving that coordination. During planning, the IO cell should facilitate coordination

between various staffs, organizations, and the MAGTF staff elements responsible for planning specific elements of IO. During execution, the cell should remain available to assist in coordination, provide support, or adjust IO efforts as necessary.

The MCPP and IO
Although the MCPP was covered in great detail in 8805A, a few notes about it here are essential to ensure that all understand how IO fits within the process. The MCPP is a six-step process, briefly portrayed and described as follows with applicable IO emphasis.
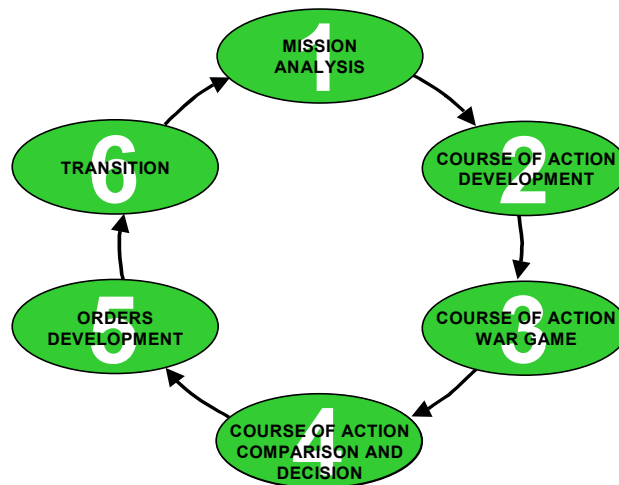
The Marine Corps Planning Process.

1. Mission Analysis. This first step's purpose is to review and analyze orders, guidance, and other information provided by higher headquarters and to produce a unit mission statement. The higher headquarters order is analyzed to extract IO planning guidance such as constraints, restraints, and planning factors. This guidance establishes the boundaries for IO planning, identifies target limitations based on policy and rules of engagement (ROE), and helps reduce the uncertainty associated with IO planning. IPB products relevant to further IO planning are developed or requested. Enemy centers of gravity (COGs) are determined. Potential risks and friendly vulnerabilities are also identified for defensive IO action. Friendly IO assets and capabilities, either organic or supporting the MAGTF as well as additional IO force structure requirements, are identified. The IO cell must fully participate in MAGTF planning activities and coordinate its planning efforts with those of the MAGTF future operations section. The most critical element to address during mission analysis is the integration of IO into the commander's vision of shaping actions.

2. Course of Action Development. During this second step, planners use the mission statement (which includes the higher headquarters commander's tasking and intent), the commander's intent, and the commander's planning guidance to develop courses of action (COAs). The IO cell will conduct an assessment of friendly vulnerabilities to enemy IO actions. The IO cell will also continue to refine its analysis of the enemy COG to determine the critical enemy vulnerabilities most susceptible to IO for use in development of initial COAs. The IO cell will closely follow the development of the OPT COAs to ensure that the IO concept of support

adequately supports these COAs. The IO cell may formulate an IO concept of support that will identify IO actions to be implemented regardless of the eventual COA that is adopted.

3. Course of Action War Game. This third step involves a detailed assessment of each COA as it pertains to the enemy and the battlespace. Each friendly COA is wargamed against selected threat COAs and will identify branches and potential sequels. The IO cell participates fully in the COA war game to refine and validate both the overall IO concept of support as well as the specific IO concepts of support for each COA. The IO actions are integrated into the COA war game in an interactive process to determine the impact on both friendly and enemy capabilities. It should also identify possible branches and potential sequels in the IO concept for further planning.

4. Course of Action Comparison and Decision. The commander, during this fourth step, evaluates all friendly COAs against established criteria, evaluates them against each other, and selects the COA that will best accomplish the mission. The IO cell is responsible for ensuring that the impact and anticipated effect of IO actions upon the enemy for each COA, and the relative merit of each COA, from an IO perspective, are provided to the commander.

5. Orders Development. In the fifth step, the staff uses the commander's COA decision, mission statement, and commander's intent and guidance to develop orders that direct unit actions. The IO cell is responsible for taking the overall IO concept of support and the concept of support specific to the COA selected by the commander and turning them into appropriate sections of the OPORD under the direction of the MAGTF IO officer. During orders reconciliation and crosswalk, the IO cell may be called upon to review the IO sections of the orders, identify gaps in planning or discrepancies, and provide corrective action. Because IO is multi-disciplined, it is found in various portions of the MAGTF OPORD.

6. Transition. The final step is the orderly handover of a plan or order as it is passed to those tasked with execution of the operation. The IO cell remains intact during the transition from planning to execution and continues to support both current and future operations. During the confirmation brief, the IO cell will ensure that the IO-capable units address their tasked IO actions as part of their overall plan to identify any remaining discrepancies or gaps in planning.

Lesson Summary

We have examined IO and its planning aspects in this lesson. Some say there is nothing new with IO and it is just a new term for a variety of functions we have always traditionally performed. Others contend that this area of warfare is "too hard." Regardless of what side of the fence you sit on, the information age is upon us and is here to stay, growing in leaps and bounds. IO will increasingly become more important in our military functions as we strive to incorporate our military might with and into other aspects of national power to achieve our national goals and objectives. Use, exploitation, and protection of information are essential for us to retain our place as a world leader facing a multitude of new threats across the globe.

JPME Summary

AREA 1					AREA 2				AREA 3					AREA 4					AREA 5			
A	B	C	D	E	A	B	C	D	A	B	C	D	E	A	B	C	D	E	A	B	C	D
X				X	X			X	X				X	X				X	X	X	X	X